REMARKS

The present application was filed on June 20, 2003 with claims 1-16.

In the outstanding Office Action dated January 16, 2007, the Examiner: (i) rejected claims 8 and 16 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,697,488 (hereinafter "Cramer"); (ii) rejected claims 1, 2, 4-6, 9, 10 and 12-14 under 35 U.S.C.§103(a) as being unpatentable over Cramer in view of U.S. Patent No. 5, 515, 441 (hereinafter "Faucher"); and (iii) rejected claims 3, 7, 11 and 15 under 35 U.S.C.§103(a) as being unpatentable over Cramer and Faucher in view of a Cramer et al. article entitled "Multiparty Computation from Threshold Homomorphic Encryption" (hereinafter "Cramer paper").

In this response, Applicant amends independent claims 8 and 16. Applicant respectfully requests reconsideration of the present application in view of the amendments above and remarks below.

Amended claims 8 and 16, which recite limitations from the perspective of the device providing assistance to the decrypting device, have been amended similar to previously amended claims 1 and 9.

Previously amended claim 1 is directed to a method for use in a device associated with a first party for decrypting a ciphertext according to a Cramer-Shoup based encryption scheme, the method comprising the steps of: obtaining the ciphertext in the first party device sent from a device associated with a second party; and generating in the first party device a plaintext corresponding to the ciphertext based on assistance from the second party device, wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device, the plaintext representing a result of the decryption according to the Cramer-Shoup based encryption scheme.

With regard to the §103(a) rejections, Applicant initially notes that a proper case of obviousness requires that the cited references when combined must "teach or suggest all the claim limitations," and that there be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine the references or

to modify the reference teachings. See Manual of Patent Examining Procedure (MPEP), Eighth Edition, August 2001, §706.02(j).

Applicant submits that the Examiner has failed to establish a proper case of obviousness in the §103(a) rejection of claims 1, 2, 4-6, 9, 10 and 12-14 over Cramer and Faucher, in that the Cramer and Faucher references, even if assumed to be combinable, fail to teach or suggest all the claim limitations, and in that no cogent motivation has been identified for combining the references or modifying the reference teachings to reach the claimed invention.

The present invention provides an efficient and provably secure protocol by which two parties, respectively designated herein as "alice" (or a first party) and "bob" (or a second party), each holding a share of a Cramer-Shoup private key, can jointly decrypt a ciphertext, but such that neither alice nor bob can decrypt a ciphertext alone. By way of one example, the invention can be used for a secure distributed third-party decryption service, which requires the joint agreement by two parties to decrypt a ciphertext. For example, this may be used to provide added security to: (1) a key recovery system by law enforcement, or (2) an "offline trusted third party" system in a fair exchange protocol. Another application involves techniques by which a device that performs private key operations (signatures or decryptions) in networked applications, and whose local private key is activated with a password or PIN (personal identification number), can be immunized against offline dictionary attacks in case the device is captured. Briefly, the goal of immunization against offline attack may be achieved by involving a remote server in the device's private key computations, essentially sharing the cryptographic computation between the device and the server.

Alice and bob obtain public and secret data through a trusted initialization procedure. After initialization, communication between alice and bob occurs in sessions (or decryption protocol runs), one per ciphertext that they decrypt together. Alice plays the role of session initiator in the decryption protocol. That is, alice receives requests to decrypt ciphertexts, and communicates with bob to decrypt these ciphertexts. We presume that each message between alice and bob is implicitly labeled with an identifier for the session to which it belongs. Multiple decryption sessions may be executed concurrently.

The Examiner in formulating the §103(a) rejection of claim 1 argues that each and every one of the above-noted limitations is met by the collective teachings of Cramer and Faucher. Below, Applicant explains how such portions of Cramer and Faucher fail to teach or suggest what the Examiner contends that they teach or suggest. While Applicant may refer from time to time to each reference alone in describing its deficiencies, it is to be understood that such arguments are intended to point out the overall deficiency of the cited combination.

Although Cramer at column 8, lines 25-35 refers to two devices, a sending device and a receiving device, the relied-upon portion of Cramer does not meet certain limitations of amended claim 1 as alleged. Cramer, at column 8, lines 25-35 states the following, with emphasis supplied:

> The computed ciphertext 30 with the cipher-number u_1, u_2, e, v is transmittable via an insecure channel, as described above. For the sake of clarity, this is not indicated in section III in FIG. 2. The ciphertext 30 does not leak any information about the keys and therefore the plaintext m is hidden assuming the Decisional Diffie-Hellman problem, also referred to as DDH problem, is hard. For the transmission of the ciphertext 30, the sending device, e.g. the first device 1 as described with reference to FIGS. 1a and 1b, uses output means, whereas the receiving devices, e.g. the second device 2 as described with reference to FIGS. 1a and 1b, uses input means for receiving the ciphertext 30.

Although the Examiner points to column 8 through column 10, line 5 as teaching or suggesting the generating step, the only reference to an exchange of information between the first and second devices is in the above quoted portion of Cramer, at column 8, lines 25-35. However, the relied-upon portion of Cramer discloses the two devices, the sending and receiving devices, interact solely to transmit the ciphertext from the sending device to the receiving devices. No where does Cramer teach or suggest the recited limitation of "generating in the first party device a plaintext corresponding to the ciphertext based on assistance from the second party device, wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device. Again, as noted-above, the first and second devices can jointly decrypt a ciphertext, but neither can decrypt a ciphertext alone, such that the first and second devices communicate with each other to decrypt the ciphertexts, which Cramer does not disclose.

The Examiner looks to the Faucher reference to supplement the above-noted deficiencies of Cramer as applied to claim 1. Although Faucher in FIG. 1 and at column 3, lines 5-50 refers to two devices, Alice and Bob, where Alice sends p, x and Y_A to Bob's cryptovariable generator 202 to compute Y_B, which Bob sends to Alice's cryptovariable generator 102, the information sent between Alice and Bob does not teach or suggest the step of generating in Alice a plaintext corresponding to the ciphertext based on assistance from Bob, wherein the assistance comprises an exchange of information between the Alice and Bob separate from the sending of the ciphertext from the second party device to the first party device, the plaintext represents a result of the decryption according to the Cramer-Shoup based encryption scheme. Instead, the information exchanged between Alice and Bob is for activating cryptographic devices 103 and 203. Upon activating cryptographic devices 103 and 203, cryptographic devices 103 and 203, under control of cryptovariable cv together encrypt plaintext P into ciphertext for transmission on insecure channel 3, and decrypt ciphertext C received from channel 3 to plaintext P.

The Faucher reference fails to supplement the above-noted deficiencies of Cramer as applied to claim 1. Accordingly, it is believed that the combined teachings of Cramer and Faucher fail to meet the limitations of claim 1.

Also, the Examiner has failed to identify a cogent motivation for combining Cramer and Faucher in the manner proposed. The Examiner provides the following statement of motivation beginning at page 5, first full paragraph of the Office Action:

> Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Faucher's reference within Cramer to include wherein the assistance comprises an exchange of information between the first party device and the second party device separate from the sending of the ciphertext from the second party device to the first party device. One of ordinary skill in the art would have been motivated to do this because it would secure communications conducted over insecure channels using public-keys method (col. 1, lines 13-15).

Applicant respectfully submits that this is a conclusory statement of the sort rejected by both the Federal Circuit and the U.S. Supreme Court. See KSR v. Teleflex, No. 13-1450, slip. op. at 14

(U.S., Apr. 30, 2007), quoting In re Kahn, 441 F. 3d 977, 988 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness."). There has been no showing in the present §103(a) rejection of claim 1 of objective evidence of record that would motivate one skilled in the art to combine Cramer and Faucher to produce the particular limitations in question. The above-quoted statement of motivation provided by the Examiner appears to be a conclusory statement of the type ruled insufficient in KSR v. Teleflex.

For at least these reasons, Applicant asserts that claim 1 is patentable over Cramer and Faucher.

Independent claim 9 includes limitations similar to those of claim 1, and is therefore believed allowable for reasons similar to those described above with reference to claim 1.

Dependent claims 2, 4-6, 10 and 12-14 are allowable for at least the reasons identified above with regard to claims 1 and 9. One or more of these claims are also believed to define separately-patentable subject matter over the cited art. Accordingly, withdrawal of the §103(a) rejection of claims 1, 2, 4-6, 9, 10 and 12-14 is respectfully requested.

Amended claims 8 and 16, which recite limitations from the perspective of the device providing assistance to the decrypting device, and include limitations similar to those of claim 1, are therefore believed allowable for reasons similar to those described above with reference to claim 1. Accordingly, withdrawal of the §102(e) rejection of claims 8 and 16 is respectfully requested.

With regard to the rejection of claims 3, 7, 11 and 15 as being unpatentable over Cramer and Faucher in view of Cramer paper, Applicant asserts that the Cramer paper reference fails to remedy the deficiencies described above with regard to Cramer. Thus, claims 3, 7, 11 and 15 are patentable at least by virtue of their dependency from claims 1 and 9. Claims 3, 7, 11 and 15 also recite patentable subject matter in their own right. Accordingly, withdrawal of the §103(a) rejection of claims 3, 7, 11 and 15 is respectfully requested.

In view of the above, Applicant believes that claims 1-16 are in condition for allowance, and respectfully requests withdrawal of the §102(e) and §103(a) rejections.

Respectfully submitted,

/William E. Lewis/

Date: September 26, 2007

William E. Lewis
Attorney for Applicant(s)
Reg. No. 39,274
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-2946